Cross-Domain Deterrence: Strategy in an Era of Complexity

15
July 2014

Erik Gartzke
Professor, Political Science Department, University of California, San Diego
(egartzke@ucsd.edu)

Jon Lindsay
Assistant Research Scientist, University of California Institute on Global Conflict and Cooperation
(jrlindsay@ucsd.edu)

Abstract

This paper introduces a research agenda to extend deterrence theory to address the increasing diversity of means available for coercion. Deterrence was first explicitly formulated as a strategic concept during the Cold War because defense against nuclear weapons appeared futile. Questions of resolve and credibility assumed central importance while the choice of means became secondary on the assumption that they would be nuclear, or at least would not affect deterrence success or failure. Increasing opportunities for aggression, particularly in space and cyberspace, and interdependencies among coercive options brings new urgency to the question of means. Complexity generates uncertainty, undermining both the simple logic of earlier deterrence frameworks and the credibility of policies founded on them. "Cross domain deterrence" seeks to counter threats in one arena by relying on unlike capabilities in another area where deterrence may prove more effective. How, for instance, might threats to cyberspace or space be countered by sea power or nuclear weapons, or even non-military tools such as access to markets or normative regimes? The increasing complexity of capabilities, linkages, and actors in the world poses opportunities and challenges that would benefit from an evolution of deterrence theory and practice.

This research is supported by Office of Naval Research Grant N00014-14-1-0071 and the Department of Defense Minerva Research Initiative. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the view of the Office of Naval Research.

1 Introduction

“When there is mutual fear,” Thucydides observed, “men think twice before they make aggressions on one another.”[1] Threats of punishment have been used to deter war since antiquity, but deterrence as a precise theoretical concept and a paramount element of national security policy only emerged in the nuclear era. States in the Cold War developed weapons they dared not use but which they needed to discourage aggression. A vast literature developed from the effort to understand bilateral nuclear bargaining as well as more baroque elaborations on the credibility of nuclear guarantees to allies, incentives for conventional war in the shadow of nuclear deterrence, and the reliability of command and control systems. The overriding focus of strategic theory was still rather narrow, however: the avoidance of collective nuclear suicide with a known opponent. This work produced broad consensus on the logic, if not the practice, of deterrence.[2]

The existential bargaining relationship envisioned by classical deterrence theory contrasts with the technological and political challenges of the contemporary security environment. Nuclear and conventional military forces continue to improve and proliferate even as new challenges emerge such as cyber warfare and pervasive surveillance, anti-satellite and space-based weapons, autonomous robotics (drones), information operations to shape opinions and catalyze dissent, and innovations still barely imagined. Some of these developments carry the potential for extremely disruptive effects on par with weapons of mass destruction, but many of them open up options for lower intensity or even nonlethal effects. A wide range of political actors may have the ability or motivation to exploit emerging capabilities, from rising powers like China to regional spoilers like

[1] Jowett 1900, §4.62

[2] Freedman 2004 notes “how complicated a theoretical tangle developed around deterrence even during the cold war, a period of unusual clarity and continuity in international affairs” (117). Classic works include Wohlstetter 1958; Brodie 1959, Kahn 1960, Schelling 1960 and 1966, Snyder 1961, Jervis 1976, 1989, Waltz 1979. Reviews of this literature include Kaplan 1983, Trachtenberg 1991, Freedman 1986 and 2004, Long 2008.

Russia or Iran, domestic factions of weak allies like Pakistan and Iraq, anarchist movements like Anonymous or terrorist groups, and the list goes on. The resulting complexity of means, linkages between them, and actors with access to them need not necessarily result in greater absolute levels of danger, but it does present numerous theoretical and practical challenges.[3] Complexity itself has become a strategic problem.

Complexity can create confusion, but also opportunities. Some of the confusion arises from uncertainty about whether new opportunities advantage stronger or weaker actors, status quo hegemons or rising challengers, nation states or lone terrorists, etc. It is possible that great powers with more experience and resources will be able to better integrate emerging capabilities to augment and enhance their power. It is also possible, and widely feared, that emerging threats crossing over established jurisdictional, environmental, or conceptual boundaries can undermine conventional military advantages, or even undermine a national nuclear deterrent. Real and imagined threats range across traditional physical environments (land, sea, air, and space) as well as the artificial construct of cyberspace, all described as war-fighting “domains” by the Pentagon. The notion of a “domain” can also be considered more generally in terms of policy jurisdiction, infrastructure ownership, command authority, or arenas of technocratic expertise. Indeed, in the extreme, each new capability or tactic involves an area of application and each interacts with existing friendly and enemy capabilities to augment or possibly degrade these capabilities. Domains are as much convenient categories for conceptualization, debate and training as discrete places with clearly delineated boundaries. For our purposes we focus on a domain as a pathway or means for coercion that is different from other means in important respects so that one may

[3] For a survey of emerging and potential threats see National Intelligence Council 2012

compare interactions between actors according to how “like” confronts “like” and, increasingly, how “unlike” confronts “unlike.”

The mobilization of capabilities in one domain to counter those in another, e.g., using air power to retaliate for terrorism or cyber disruption of military command and control, are “cross domain” interactions. By extension, “Cross domain deterrence” (CDD) involves using capabilities of one type to counter threats or combinations of threats of another type, in order to prevent unacceptable attacks. Warnings by U.S. policymakers that response to a destructive cyber attacks need not be limited to the cyber domain but might also include conventional or even nuclear punishment are examples of CDD.[4] Efficient CDD consists of using advantages in one domain or area to cover disadvantages in another, shifting the terms of the bargain and making the best use of one’s comparative advantages to optimally deter threats in areas where one is confronted by comparative or even absolute disadvantage. Unfortunately, the strategic implications of complex linkages between actions and effects across boundaries—the potential for escalation, the interpretation of signals, even the effects of operations—are as yet still poorly understood. To compound the confusion, policymakers may not yet know how their own governments will respond to unconventional attacks. Tremendous uncertainty in the current and future threat environment, together with the practical challenges of integrating diverse instruments of power across domains, makes CDD a daunting problem. At the same time, the potential advantages of doing CDD well, or at least better, are substantial.

[4] E.g., Deputy Secretary of Defense William J. Lynn, III, stated that “the United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place of our choosing.” July 14, 2011; http://www.defense.gov/speeches/speech.aspx?speechid=1593. Similarly, Secretary of Defense Leon Panetta stated, “there's no question that if a cyber attack… crippled our power grid in this country, took down our financial systems, took down our government systems, that that would constitute an act of war.” May 27. 2012; http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5041

The first decade of the twenty-first century raised the problem of CDD to prominence in the U.S. defense policy community. In 2007 China's use of a ground-based interceptor to destroy one of its derelict communications satellites highlighted the vulnerability of vital U.S. military and commercial spacecraft and raised thorny questions about the risks of misinterpretation and escalation with China. Growing Chinese assertiveness in East Asia and the nuclearization of the Korean peninsula led to renewed scrutiny of American extended deterrence guarantees to regional allies, even as Chinese military modernization seeks to counter American power projection through asymmetric "anti-access, area denial" initiatives. The discovery of the Stuxnet worm in 2010 and ensuing revelation of the Olympic Games program (allegedly a covert collaboration of the U.S. and Israel to sabotage the Iranian nuclear program) demonstrated that cyber risks need not be limited to the internet but also threaten physical destruction of industrial infrastructure. Olympic Games leveraged novel covert options to supplement overt diplomatic sanctions and tacit threats of airstrikes to pressure Iran to eschew proliferation (although the strategic impact of this sabotage remains ambiguous insofar as Iran continued to enrich uranium and develop its own cyber warfare capacities). The ongoing standoff between Russia and NATO over Ukraine has witnessed Russian use of subversion and information operations to facilitate the annexation of Crimea and NATO Allies' use of financial sanctions and airpower reinforcements to deter further encroachment. None of these events created a decisive shift in the political order, and some even reinforced it. Yet they raised the specter of more disruptive threats on the horizon, and they prompted U.S. policymakers and defense analysts to search for potential responses. Could U.S. cyber and space vulnerabilities undermine the credibility of the nuclear deterrent? Might nuclear or other threats deter catastrophic attacks on cyber and satellite infrastructure? How should the U.S. tailor deterrence to cross domain threats posed by China, Iran, North Korea, Russia, or even non-state actors? Would foreign adversaries interpret CDD signals the way the United States intends them and what are the implications if they do not?

This paper triangulates and refines the notion of CDD. What is CDD and how does it work? We first situate the need for CDD in the historical evolution of complexity in the means of coercion. We also clarify the historical continuities and novelties of CDD as a concept. We then explain how CDD differs from classical deterrence. Following this, we parse the complexity of CDD into more tractable questions about threat capabilities, economic and infrastructural interdependence, and the variety of state and non-state adversaries who have access to these capabilities. In something of a surprise given the complexity of the subject matter, we are able to show that considerable intellectual terrain can be productively surveyed and mastered with relatively simple conceptual tools.

2 Expanding the Means of Coercion

In the aftermath of Hiroshima, as Bernard Brodie famously pointed out, nuclear weapons made war fighting suicidal even as they facilitated strategic deterrence. With intercontinental missiles, survivable submarines, and massive arsenals, defense against nuclear weapons was impossible, or at least prohibitively risky. Strategists turned instead to deterrence and articulated its logic in detail. Deterrence was not a new phenomenon, but the demand for theory about it was new. CDD is also not new. Strategic actors have long combined capabilities or shifted domains to make coercive threats or counter them. The Greeks responded to the abduction of Helen of Troy with a siege rather than counter-abductions. The stalemate of symmetric confrontation outside the gates of Troy ended with the ruse of the Trojan Horse and its Hellenic commandos. The British sank the French fleet in the Battle of the Nile rather than attempting to directly confront Napoleon’s army on land in Egypt. The United States deployed a naval blockade and used the threat of nuclear escalation to force the Soviet Union to reconsider its deployment of missiles to Cuba. Sun Zi recognized that deception was essential to the art of war long before Chinese hackers began sending phishing emails to American defense contractors. As with deterrence in general before the advent of nuclear weapons, CDD has long been seen as either sufficiently intuitive in practice or so dense in abstract that there was no perceived need (or willingness) to articulate an explicit theory. The logic of CDD has thus not yet been worked out by practitioners or analysts.

Evolution in the technology and application of influence necessitates an expansion of deterrence theory. **Error! Reference source not found.** displays a rough timeline of the emergence of important military technologies over the past century and a half.[5] None of these technologies produced a revolution in warfare on their own, with the possible exception of nuclear weapons.[6] The literature on military innovation has reached a strong consensus that technological innovation in itself does not determine military outcomes without the development of complementary doctrines and organizations to employ it.[7] Yet this literature tends to examine innovation and adoption of specific technologies, often in specific cases, rather than assessing the cumulative increase in complexity of these innovations taken together. Each introduction of a new capability in **Error! Reference source not found.** created a new tactical or strategic option for militaries, and there has been plenty of improvement in the efficacy of each of these options since their initial battlefield debut. Improvements in technology and employment accrue to both the offense and defense, so that the performance implications in any given instance are ambiguous. Even so, performance has more often than not required the mastery of a deeper and wider division of labor. A great jump in complexity occurs at the cusp of the twentieth century with the thorough

[5] This is a very rough initial survey of the adoption of military technology intended to illustrate increasing complexity. It shows an approximate date of military adoption of a given technology and its continuing utility.

[6] For dissent on the Nuclear Revolution thesis see Gavin 2012.

[7] Inter alia, Rosen, Knox & Murray, Biddle, Grissom

industrial mechanization of war, and innovations have continued to expand the range of coercive technologies throughout the late industrial era up to the present. There is no reason to expect this trend to abate any time soon.[8]

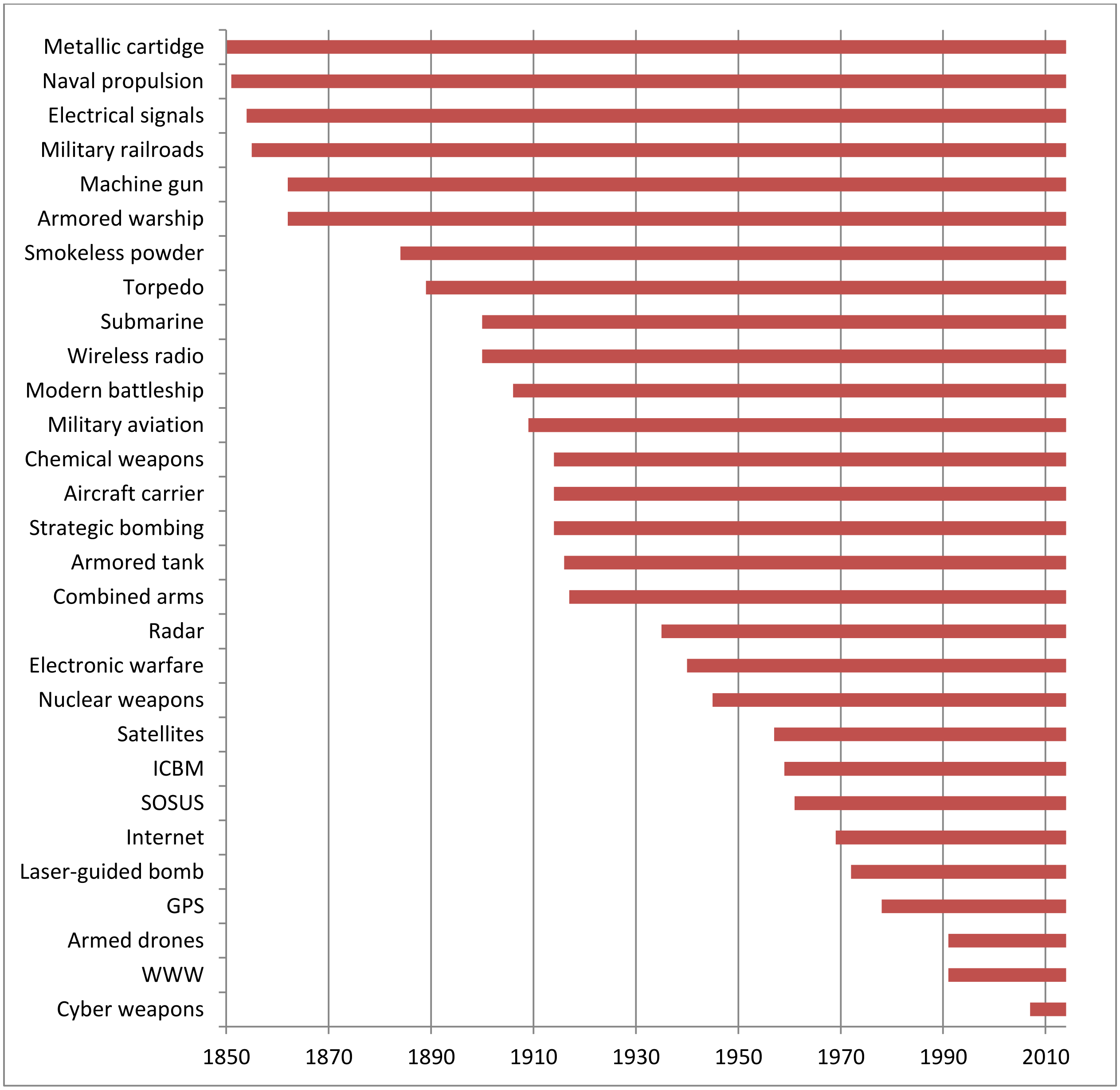

Figure 1: Emergence of important military technologies

[8] We are on the increasing tip of the "hockey stick" of industrial innovation and change. Nothing grows exponentially forever, of course. The top of the S-curve in this phase of macro-evolutionary "punctuated equilibrium" is still ahead of us. That new long-term steady state—or maybe systemic collapse—will no doubt introduce different strategic challenges. But we're not there yet.

A sustained rise in socio-technical complexity is widely recognized to be a key historical trend in the evolution of industrial societies more broadly, increasing the ability to make money, and to make war. Industrialization increases the resources available to states and other actors, but it also necessitates the development of new institutions and technologies required to manage increasing scales of production and coordination. These changes in turn create increasing returns to the control of controls.[9] Military and economic affairs have been spurred on by a competitive ratcheting up of complexity in recent centuries. The preoccupation in the Revolution in Military Affairs (RMA) literature with emerging technologies like computer networks and autonomous robotics is in fact a reflection of the leading edge of a much more significant long term trend. It is not specific technologies or even the complementary institutions for their employment which make the difference, but the overall increase in the complexity of capabilities and the linkages among them, as well as the types of actors who exploit them. There are a growing number of ways to influence, with more emerging over time, and with complex interactions across options.

Strategy debates surrounding the introduction of new and potentially disruptive technologies often divide on the question of influence within versus across domains. These debates are most prevalent in the opening of major domains of strategic interaction. The interaction between land and sea power is perhaps one of the most prominent and established cross-domain problems in strategic history. Militaries have exploited the sea for millennia but until the sixteenth century sea battles were really just clashes of soldiers on floating, steerable islands.[10] Warships with keels and cannon introduced a whole new form of fighting and required a new sort of military

[9] Beninger 1986, and the literature on endogenous growth more generally.

[10] The front structure of a ship (near the bow) is still called a “forecastle,” strange vocabulary for something at sea.

specialist. Navies and naval warfare developed in the ensuing centuries, but maritime strategy only really emerged in the late 19th and early 20th centuries. Notably, this was a period of rapid globalization and technological change as sea power was transformed by the advent of steam propulsion, steel armor, long-range gunnery, torpedoes, wireless radio, etc. Moreover, new naval powers like Germany and Japan experimented with the new technology, posing challenges to more established sea powers like Britain and the United States. This technological and political ferment inspired a new generation of maritime strategists, foremost among them the American Alfred Thayer Mahan and the Englishman Julian Corbett. Both Mahan and Corbett emphasized the critical importance of the sea for the economic vitality of a nation, meaning that sea power was inherently a cross domain concept with utility in both peace and war and with implications for prosperity ashore. Yet these two naval strategists espoused quite different views of the proper use of sea power. Mahan emphasized the control of sea lines of communication and advocated the concentration of the fleet to destroy the enemy fleet. Corbett by contrast focused on more circumspect uses of sea power to influence operations ashore, through naval blockades, commerce raiding, and expeditionary warfare. Thus Mahan focused on the transformative power of technology in one particular domain, whereas Corbett focused on the complementary aspects of power in multiple domains and laid particular emphasis on the use of any naval or military instruments to serve national political interests.

These debates were recapitulated with other major technological developments and the emergence of other nominal domains. Some early advocates for air power argued that strategic bombers would be able to render land (and sea) power obsolete by flying over the battlefield directly to destroy the moral or economic capacity of the enemy to wage war. Other aviation strategists pointed to close air support and other modes of tactical aviation which complement, rather than substitute for, land (and naval) elements. Likewise in the contemporary cyber debate, one perspective focuses on the paralyzing menace of a “digital Pearl Harbor” where wars are fought and won in cyberspace alone, while others see a more long term espionage contest with the potential to cause a “death by a thousand cuts,” influencing the ability of a target to compete over the longer term in other economic and military arenas. Every new domain of influence raises similar questions about who benefits and inevitably creates debates about the relationship between novel and existing capabilities. The conceptual problems housed within the rubric of CDD have thus been developing for well over a century. We believe that it is time to recognize and characterize the more general strategic implications of this increase in coercive potential rather than recapitulating the same debate with the emergence of each new domain.

An ability to manage complexity has become increasingly critical in military affairs with each passing decade of the modern era. The emergence of combined arms warfare (or what Stephen Biddle calls “the modern system”) during the First World War enabled military organizations to restore movement to an increasingly lethal battlefield.[11] Combined arms warfare works by using the advantages of one category of force to cover the weaknesses of another. The advantage of infantry is its ability to identify targets in the close fight, but soldiers are vulnerable in the open. Armor can provide fires and protection, even as it is vulnerable to other arms such as artillery and tactical aviation. Similarly, a naval carrier battle group uses different classes of ships, submarines, and aircraft to project power against even formidable technological defenses afloat and ashore. The combination of cover, concealment, movement, suppressive fire, tactical initiative, and cooperation amongst branches and services made the modern system of offense especially effective on the highly lethal battlefields of the twentieth century. Yet adoption and eventual

[11] Biddle 2004

diffusion of this innovation in strategy and organization lagged the introduction of technology. Enormous challenges were involved in mastering the inherent complexity and in accumulating the human and organizational capital required for combined arms warfare. Another form of complexity management complements and enables force employment complexity, namely the engineering systems integration needed to design and field sophisticated weaponry.

The military and industrial foundations of American hegemony in the mid-twentieth and early twenty-first century lie in the ability to master both types of complexity, fielding a complex panoply of weapons and developing the sophisticated organizations capable of creating a productive synthesis of multiple technologies to project power around the globe. Barry Posen describes U.S. mastery of air, sea, and space operations as "command of the commons," limited only by "contested zones" on the ground where more committed adversaries can survive the lethality of American attention and impose costs.[12] In other words, the coercive advantage of the United States is founded on its ability to integrate military and economic instruments across domains. This brings us back to the problem we began with, whether American cross-domain prowess is being undermined by emerging developments in space, cyberspace, and other socio-technical arenas that might advantage its adversaries. One way to think about the challenge of CDD is analogous to the problem that combined arms warfare addresses tactically, and increasingly strategically, but applied now and in the future to the grand strategic level. What combination of instruments and activities improve or preserve command for the actors who have it, and what combinations serve to enhance the ability to contest command for those who don't?

[12] Posen 2003, Posen 2014

3 Toward a Logic of Cross Domain Deterrence

Deterrence theory rests on the notion of political bargaining between broadly rational actors. It is desirable to retain this paradigm, at least for the present.[13] Like classical deterrence, a theory of CDD should link the technical ability to harm with the political utility of aggression. Unfortunately, most of the discussion of CDD and associated challenges in cyberspace, space or elsewhere tends to focus on the technological "cross domain" problem rather than on the strategic "deterrence" problem. Considerable attention has been given to the expanding frontier of novel threats against which the U.S. and other nations must defend as a result of the eroding global commons, new offensive capabilities, pervasive interconnectivity, etc.[14] Defense policymakers have also begun to explore the considerable practical challenges of optimizing cross domain responses at the operational level of war, e.g., in the U.S. "AirSea Battle" concept to respond to Chinese area denial and new bureaucratic constructs like U.S. Cyber Command.[15] Less attention has been devoted to the strategic logic underpinning the behavior of different actors with novel threats, i.e., how leaders and commanders link means and ends to achieve their best advantage.

Deterrence, by definition, involves the use of threats to dissuade adversaries from taking unwanted action. An effective deterrent policy must send a clear and predictable message: "cross this boundary and expect these consequences." Uncertainty about the parameters of the boundary, the nature of the punishment, the credibility of the threat, or reassurance that compliance will avoid punishment each diminish the potency of deterrence. Ambiguity can improve deterrence only in cases where the credibility of an extreme consequence like mutual nuclear suicide is inherently

[13] It is possible to take a different position about how humans perceive and reason. This has not been practiced widely with classical deterrence, in part because deterrence theory relies on the notion of a motivating quid pro quo. We are certainly not opposed to exploring the implications of non-rational agency, but this complicates the concept for now and makes it more difficult to connect our work with classical theory without clearly improving predictions.

[14] Representative surveys include Jasper 2010, Denmark and Mulvenon 2010

[15] Inter alia, Schwartz and Greenert 2011; van Tol et al 2010; Lynn 2010

dubious and must be bolstered by some probabilistic risk of unintended accident. Schelling's "threat that leaves something to chance" thus allows the coercer to heighten the risk of an undesirable outcome that it can't rationally choose with certainty.[16] While a predictable deterrent policy does not guarantee success—a challenger may still value the expected political gains of an action over the potential risk of punishment—a policy that does not enable opponents to predict the national response makes deterrence failure much more likely.

Effective CDD strategies would seek to restore the credibility of deterrent threats as challengers develop new ways to evade existing deterrence regimes. CDD can and should look to familiar deterrence principles. What differs is the technological and political context of bargaining. Traditional deterrence theory is agnostic about means (usually assuming the means are nuclear), but choice among means is essential for CDD. The possible combinations of threat capabilities, infrastructural and institutional linkages, and actors with various motivations to act or to be deterred by a given threat generate uncertainty that itself becomes a critical challenge.

Much scholarship on deterrence still focuses primarily on nuclear weapons with little consideration of the interaction between other means of influence (especially cyber and space, both critical for the employment of nuclear forces today and which, many believe, may offer strategic substitutes for nuclear capabilities in some circumstances).[17] The literature on the interaction between nuclear and conventional forces offers some useful starting points, for instance the idea that nuclear stability could incentivize conventional instability.[18] Similarly, because cross-domain capabilities considerably expand opportunities for disruption and influence rather than outright

[16] Schelling 1966
[17] E.g., Shultz et al 2011
[18] Snyder 1965

destruction, we may observe greater incidences of deterrence failure for less intense conflict even as deterrence succeeds in preventing high intensity conflict.

Many concepts from the vast body of deterrence theory have been usefully applied to non-nuclear interactions. There is an emerging literature on the problem of deterring asymmetric threats like suicide terrorists, who appear (superficially) to disregard threats of punishment.[19] Scholarship on conventional deterrence tends to focus on similarly-equipped armies facing one another on traditional battlefields rather than on more esoteric and complex combinations of cross-domain capabilities,[20] to say nothing of the potential and pitfalls of directly substituting conventional for nuclear options (as with the U.S. military Prompt Global Strike initiative).[21] Novel deterrence challenges have been explored in specific regional problems, and in countries that have different conceptions of deterrence.[22] Israel, for example, explicitly considers and expects deterrence to fail periodically against conventional and irregular threats, necessitating repeated punishment over time.[23] These national variations have not yet been pulled together and assessed in any consistent and coherent way with regard to the contemporary threat landscape.

The diverse uses of tools in multiple domains for both deterrence and war fighting, even (or especially) at very limited levels of intensity, suggests that the relationship between deterrence and compellence,[24] as well as between threats and actual uses of force, is likely to be substantially more complicated in CDD. There are a number of useful theoretical precedents to draw from in

[19] Knopf 2010; Morgan 2012

[20] Mearsheimer 1983, Slantchev 2011

[21] Stone 2012

[22] E.g., Paul et al 2011

[23] Adamsky, working paper

[24] According to Schelling 1960, deterrence is the use of threats to dissuade an adversary from taking an action in the future while compellence is the use of threats to persuade an adversary to stop an action already underway. The relationship between the two is likely to be complicated in CDD.

the vast literature on strategy, but there is also considerable new ground to explore by explicitly focusing on the persistent increase of socio-technical complexity over time.[25]

4 An Agenda for Analyzing Strategic Complexity

The fundamental problem of CDD is to navigate the combinatoric complexity of increasing capabilities, linkages, and actors. Complexity is the very problem which gives rise to CDD. Analysis of CDD should break down and make sense of this complexity. Whereas traditional deterrence theory focuses on bilateral bargaining with nuclear threats, our approach to CDD systematically relaxes three assumptions. First, it increases the range of available capabilities to make symmetric or asymmetric moves possible in the bargaining process. Second, it increases the linkages between these capabilities, to include interdependence in their production and exchange, interconnection through shared infrastructure, and the combination of capabilities in a portfolio of options. Third, it increases the number and types of actors to consider balancing, alliances and extended deterrence, principal-agency and other contracting relationships. These relaxations can be analyzed separately and then synthesized subsequently.

In policy discourse on CDD we can discern some emerging conventional wisdom in each of these three relaxations. These fashionable yet inchoate ideas provide us with a jumping off point from which to develop a much more general, analytically rigorous, and empirically testable theoretical framework. Existing points of departure also help to ensure that the fruits of basic scientific research are nevertheless capable of yielding implications with direct policy relevance.

[25] The term “sociotechnical” refers to the interdependent relations between technical engineering and social institutional factors in any given system. See Hughes 2004, Nye 2006.

Table 1: Contrasting expectations about the effect of complexity on strategy

	Relevance to CDD	**Conventional Wisdom**
Capabilities	Emerging capabilities provide (or undermine) a differential advantage to actors at different scales	Asymmetry provides advantage to weaker challengers over stronger incumbents
Linkages	Complicated interdependencies across domains and infrastructures magnify (or dampen) vulnerabilities to asymmetric threats	Interdependent markets and infrastructures are systematically vulnerable to catastrophic shock
Actors	A wide variety of political actors may (or may not) derive political advantage from asymmetric capabilities and interdependent systems	Multilateral proliferation of cross domain capabilities to and interaction among threat actors generates instability

The three dimensions of complexity in Table 1 are strongly affected but not uniquely determined by emerging technologies. By emphasizing political systems in our analysis, we can better avoid the trap of technological determinism which has, to date, plagued early discussions of CDD. Strategic dangers have often been inferred directly from technological possibilities (e.g., the claim that because cyber tools can in principle attack electrical power grids, cyber-war with states or terrorists is imminent). However, technology does not by itself determine new strategic or tactical outcomes. Innovations such as sophisticated hacking methods, complex critical infrastructures, and global supply chains (among others) clearly shape the political constraints and opportunities facing state and non-state actors. Yet the effects of technology on strategy and conflict are usually highly contingent on the political and institutional circumstances of the actors who seek to exploit evolving technology in order to pursue a variety of interests.[26]

There already exists a rich social science literature to draw upon in each of the three areas above. Questions about capabilities, linkages, and actors are hardly new, and in many ways are the conceptual core of political science. Indeed, a key component of efficient research is to leverage existing concepts so there is no need for researchers to start from scratch or "reinvent the wheel."

[26] For general criticism of technological determinism, the idea that social consequences flow straightforwardly from technical innovation, see Smith and Marx 1994; Mackenzie, 1993.

What is new is the integration of each concept and accompanying knowledge into a common scientific research program for CDD. These interrelated concepts should build on one another in a modular yet cumulative process. Modularity enables us to isolate important factors and mechanisms. The cumulation of knowledge allows us to apply the insights gained in one stage to the next. Table 2 summarizes this approach by highlighting research questions at the technical/operational and political/strategic levels. As discussed previously, these must be distinguished in terms of technical possibility and bargaining utility in order to avoid technological determinism and to emphasize the political roots of objective and in strategy.

Table 2: Research Questions by Attributes of Complexity and Levels of Analysis

	Operational Questions	**Strategic Questions**
Capabilities	• What are the important characteristics of emerging threat technologies? • What are their resource and human capital requirements for design and use? • Does the diffusion of capabilities harmonize or separate actors?	• How do bargaining dynamics differ among various combinations of strong and weak actors? • How does crisis stability and instability vary with mixes of capabilities? • Are asymmetric capabilities escalatory or de-escalatory?
Linkages	• What types of interdependencies create vulnerabilities or resilience? • Are resources fungible across domains (political, military, economic)? • Are interdependent systems fragile or resilient?	• How does interdependence promote or shift advantages of offense relative to defense? • Does interdependence create incentives to move first or show restraint? • How do actors shift their advantages across interdependent domains?
Actors	• Which actors have the doctrine and ability to exploit which asymmetries and interdependencies? • What stakeholder coordination challenges exist in cross-domain operations (Public-private, domestic-international)? • How do competitors work by, with, and through third parties, and what principal-agent problems and solutions emerge?	• How effective are alliance and wedge strategies in a cross-domain world? • How do multi-polar cross-domain interactions affect the frequency and intensity of war? • Where and when in a complex political geography should we expect cross-domain conflict to escalate, even to nuclear war?

Research into CDD should develop analytically rigorous theory to answer these questions and to begin the process of empirical and computational evaluation. Systematic investigation can progressively increase complexity by multiplying the asymmetric capabilities available, types of relationships connecting actors, and the number of actors engaged. Yet beyond a few actors and relationships interactions become too complex and convoluted to deal with analytically. Indeed, we do not want overly complex theory, particularly given the complexity of subjects and relationships already in the problem of CDD, since the object is to clarify and make practical the application of key insights. At the same time complexity implies an even greater need for careful empirical assessment, to ensure that theory is a valid and to assess the potency of predictions.

Empirical assessment in a period of transition is strained by the need to infer from incomplete data or from imperfect analogies. We advocate the pursuit of two complementary and overlapping strategies. First, to the degree possible, we can use the past to predict the future, basing assessments of the drivers of CDD on contexts and behaviors that have already come to pass. The increasing complexity of combined arms warfare is one such example. We can also assess the effects of asymmetry, interdependence and multi-polarity separately, and in some cases jointly, on existing interstate conflict data (wars, disputes, crises, and armed conflicts) covering the universe of interstate cases and extending back to 1816. A second strategy is to simulate complex bargaining among actors, extrapolating from historical data, in order to better understand the nature and evolultion of dynamics in dyadic, regional and system behavior.

Considerable information is already available about the causes of war and peace among nations and between states and non-state actors that can be applied in the context of CDD. Extensive qualitative and quantitative studies have examined factors like regime type, proximity, capabilities, wealth, trade and other variables. These data and insights can form the backdrop for our tests. The trick, as always, is not to examine everything, but to develop tests in a context where results are indicative. It is highly unlikely that *everything* will be different in the future. Indeed, our view of CDD, as we have already implied, is that it is the fruition of processes that have been developing and increasing in salience over many centuries. The fact that they have now become important enough to be the focus of analytical and operational analysis, rather than treated as "noise" is simply evidence of their maturation, not their discontinuity from the past.

The basic "bricks and mortar" of our theoretical perspective is again in reach by conceiving of social institutions as a type of bargaining equilibrium between agents in a political system and war as a type of bargaining failure. There are countless institutions which regulate social behavior in any system, some formal and some informal. When novel technological and political developments alter participants' bargaining power, actors may be tempted to renegotiate; renegotiation can lead to war.[27] The disruptive technologies of CDD which affect capabilities, linkages, and actors are precisely the kinds of developments destined to prompt bargaining failures. Therefore, by analyzing complex bargaining directly in our exploration of CDD, we have the potential to show how conflicts at different scales are related, perhaps through relationships of restraint rooted in interdependence or escalatory spirals.

5 Why CDD? Why Now?

The world is steadily growing more complex, and CDD is becoming more relevant. Because of increasing means for coercion and the uncertainty the resulting complexity creates, a conceptual understanding of CDD has become a limiting factor for national security strategy. It is easier to fund technology for offense or defense than to understand incentives and even strategy. The

[27] Wagner 2007

complexity of these technologies makes their strategic implications ever harder to comprehend. China’s rise makes CDD particularly salient, but it also matters for relations with Russia, Iran, North Korea, and NATO, to say nothing of non-governmental organizations. Yet if CDD is becoming harder, the advantages that stem from getting it right are growing exponentially.

A natural question to ask is whether CDD is fundamentally destabilizing. Many people certainly think so. Emerging technologies seem, by some accounts, to advantage opportunistic attackers, weaker actors, and challenges to the status quo. Interdependent infrastructures create grave vulnerabilities for all, especially the most advanced industrialized states. The growing number of potential threats from ever more state and non-state actors complicates the choice of strategy. However, the opposite might be the case. Some asymmetric capabilities reinforce the status quo, while economic interdependene, a form of complexity common in recent times, is generally thought to be pacifying. More and more actors have a stake in the current system. We need better theory and policy approaches to resolve or at least clarify these controversies.

In short, this research program asks how increasing technological and political complexity affects coercive strategy. What pitfalls and opportunities does CDD offer as deterrence can be pursued in an ever greater number of ways? What is the strategic logic of CDD, even for domains that have yet to be invented (or imagined)? The basic challenge of the research project is to render the increasing complexity of CDD analytically tractable.

CDD is an emerging contemporary defense policy problem that appears destined to have major implications for the future in thinking about deterrence and military operations. Just as mastering combined arms operations assigned “winners” in combat in the twentieth century and allowed the United States to wield an affordable and effective form of dominance as hegemon, so too making sense of CDD will allow some actors to exercise influence in the future. Given that global complexity is continually increasing, successful CDD will become even more critical and challenging. Declining U.S. defense budgets elevate the importance of strategy: while the U.S. cannot afford to defend everywhere, it can still deter. There will be technological changes that create new threats in the future that are hard to imagine now; instead of reacting piecemeal to each new threat or capability, a strategic policy designed explicitly to confront the problem of continuously increasing socio-technical complexity would make it easier to accommodate, even anticipate, novel threats. To design such a strategy, policymakers must make sense of CDD. The question is whether they will be forced to do so intuitively or whether they can be guided by a theoretically-grounded strategic logic.

6 Works Cited

Adams, Karen Ruth. 2003. Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance. International Security 28(3): 45-83.

Agar, Michael H. 1996. The Professional Stranger: An Informal Introduction to Ethnography, 2nd Edition. New York, NY: Elsevier Academic Press.

Allard, C. Kenneth. 1990. Command, Control, and the Common Defense. New Haven, CT: Yale University Press.

Biddle, Stephen. 2004. Military Power: Explaining Victory and Defeat in Modern Battle. Princeton, NJ: Princeton University Press.

Boehmer, Charles, Erik Gartzke and Quan Li. 2001. Investing in the Peace: Economic Interdependence and International Conflict. International Organization 55(2):391 - 438.

Breetz, Hanna L. 2013. Fueled By Crisis: U.S. Alternative Fuels Policy, 1975-2007. Ph.D. Dissertation, MIT Department of Political Science.

Brodie, Bernard. 1959. Strategy in the Missile Age. Santa Monica, CA: RAND.

Brooks, Stephen G. 2007. Reflections on Producing Security. Security Studies 16(4): 637—678.

Cederman, Lars-Erik. 2003. Modeling the Size of Wars: From Billiard Balls to Sandpiles. American Political Science Review, 97(1): 135-150.

Charmaz, Kathy. 2006. Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis. Newbury Park, CA: Sage.

Clauset, Aaron, Maxwell Young, and Kristian Skrede Gleditsch. 2007. On the Frequency of Severe Terrorist Events. Journal of Conflict Resolution 51(1): 58 - 88.

Clauset, Aaron, and Ryan Woodard. 2012. Estimating the Historical and Future Probabilities of Large Terrorist Events. http://arxiv.org/abs/1209.0089

Collier, David, and Henry E. Brady. 2004. Rethinking Social Inquiry: Diverse Tools, Shared Standards. Rowman and Littlefield Publishers, Inc.

Creedon, Madelyn R. 2011. Space and Cyber: Shared Challenges, Shared Opportunities. Remarks to the USSTRATCOM Cyber and Space Symposium, November 15.

Denmark, Abraham M., and Dr. James Mulvenon. 2010. Contested Commons: The Future of American Power in a Multipolar World. Washington, DC: Center for a New American Security.

Deudney, Daniel H. 2006. Bounding Power: Republican Security Theory From the Polis to the Global Village. Princeton University Press.

Eriksson, Johan, and Giampiero Giacomello. 2006. The Information Revolution, Security, and International Relations: (IR)relevant Theory? International Political Science Review 27(3): 221–244.

Freedman, Lawrence. 1986. The First Two Generations of Nuclear Strategists. In Makers of Modern Strategy: From Machiavelli to the Nuclear Age, ed. Peter Paret. Princeton, NJ: Princeton University Press.

Freedman, Lawrence. 2004. Deterrence. Cambridge: Polity Press.

Gartzke, Erik. 2007. The Capitalist Peace. American Journal of Political Science. 51(1):166 - 191.

Gartzke, Erik. 2011. Interdependence Really is Complex. Typescript. University of California, San Diego.

Gartzke, Erik. 2012. Nuclear Capabilities and Conventional Conflict. Typescript. University of California, San Diego.

Gavin, Francis J. 2012. Nuclear Statecraft: History and Strategy in America's Atomic Age. Ithaca NY: Cornell University Press.

Gerson, Michael S. 2009. Conventional Deterrence in the Second Nuclear Age. Parameters.

Glaser, Barney G., and Anselm Strauss. 1967. Discovery of Grounded Theory: Strategies For Qualitative Research. Chicago, IL: Aldine Publishing Co.

Glaser, Charles L., and Chaim Kaufmann. 1998. What Is the Offense-Defense Balance and Can We Measure It? International Security 22(4): 44-82.

Hughes, Thomas P. 2004. Human-Built World: How to Think about Technology and Culture. Chicago, IL: University of Chicago Press.

Hutchins, Edwin. 1995. Cognition in the Wild. Cambridge: MIT Press.

Jasper, Scott. 2010. Securing Freedom in the Global Commons. Stanford, CA: Stanford University Press.

Jervis, Robert. 1976. Perception and Misperception in International Politics. Princeton, NJ: Princeton University Press.

Jervis, Robert. 1989. The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon. Ithaca, NY: Cornell University Press.

Jowett, Benjamin. 1900. Thucydides, translated into English, to which is prefixed an essay on inscriptions and a note on the geography of Thucydides, Second edition. Oxford: Clarendon Press.

Kahn, Herman. 1960. On Thermonuclear War. Princeton University Press.

Kaplan, Fred M. 1983. The Wizards of Armageddon. Stanford, CA: Stanford University Press.

Keohane, Robert O., and Joseph S., Jr. Nye. 2001. Power and Interdependence, 3rd Ed. New York, NY: Longman.

King, Gary, Robert O. Keohane, and Sidney Verba. 1994. Designing Social Inquiry. Princeton University Press.

Knopf, Jeffrey W. 2010. The Fourth Wave in Deterrence Research. Contemporary Security Policy 31(1): 1–33.

Krepon, Michael. 2004. The Stability-Instability Paradox, Misperception, and Escalation-Control in South Asia. In Prospects for Peace in South Asia, ed. Michael Krepon, Rodney Jones and Ziad Haider. Washington, D.C.: Stomson Center pp. 1–24.

Lawson, Sean. 2011. Beyond Cyber Doom: Cyber Attack Scenarios and the Evidence of History. George Mason University, Mercatus Center, Working Paper (11-01).

Lewis, James A. 2010. Cross-Domain Deterrence and Credible Threats. Center for Strategic and International Studies White Paper.

Libicki, Martin C. 2007. Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press.

Libicki, Martin C. 2009. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND.

Lieber, Keir A. 2000. Grasping the Technological Peace: the Offense-Defense Balance and International Security. International Security 25(1): 71-104.

Lincoln, Yvonna S., and Egon G. Guba. 1985. Naturalistic Inquiry. Newbury Park, CA: Sage.

Lindsay, Jon R. 2011. Information Friction: Information Technology and Military Performance. Ph.D. Dissertation, MIT Department of Political Science.

Lindsay, Jon. 2013. Stuxnet and the Limits of Cyber Warfare. Security Studies 22(3): 365-404.

Long, Austin. 2008. Deterrence: From Cold War to Long War: Lessons from Six Decades of RAND Research. Santa Monica, CA: RAND.

Lynn, William J. 2010. Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Affairs 89(5).

Lynn-Jones, Sean M. 1995. Offense-Defense Theory and Its Critics. Security Studies 4(4): 660-691.

Makovsky, David. 2012. The Silent Strike: How Israel Bombed a Syrian Nuclear Installation and Kept It Secret.

Manzo, Vincent. 2011. Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit? National Defense University Strategic Forum. December

Mearsheimer, John J. 1983. Conventional Deterrence. Ithaca, NY: Cornell University Press.

Morgan, Patrick M. 2012. The State of Deterrence in International Politics Today. Contemporary Security Policy 33(1): 85–107.

Nacht, Michael. 2010. Luncheon Address. Air, Space, and Cyberspace Power in The 21st Century, 38th IFPA-Fletcher Conference on National Security Strategy and Policy, January 20-21.

National Intelligence Council. 2012. Global Trends 2030: Alternative Worlds. Washington DC: Office of the Director of National Intelligence.

National Research Council. 2010. Proceedings of a Workshop on Deterring Cyberattacks. Washington, DC: National Academies Press.

Nye, David E. 2006. Technology Matters: Questions to Live With. Cambridge, MA: MIT Press.

Obama, Barack. 2012. Taking the Cyberattack Threat Seriously. Wall Street Journal (19 July).

Office of the National Counterintelligence Executive. 2011. Foreign Spies Stealing U.S. Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011.

Panetta, Leon. 2012. Remarks on Cybersecurity to the Business Executives for National Security, New York City, 11 October. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Paul, T. V., Patrick M. Morgan, and James J. Wirtz. 2007. Complex Deterrence: Strategy in the Global Age. Chicago: U Chicago.

Perrow, Charles. 1999. Normal Accidents: Living with High Risk Technologies. Princeton, NJ: Princeton University Press.

Pollpeter, Kevin. 2012. Controlling the Information Domain: Space, Cyber, and Electronic Warfare. In Ashley J. Tellis, and Travis Tanner (Eds.), Strategic Asia 2012-13: China’s Military Challenge. Seattle, WA: National Bureau of Asian Research.

Powell, Robert. 1999. In the Shadow of Power: States and Strategies in International Politics. Princeton NJ: Princeton University Press.

Russett, Bruce, and John Oneal. 2001. Triangulating Peace: Democracy, Interdependence, and International Organization. New York: W.W. Norton and Co.

Sagan, Scott D. 1993. The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton University Press.

Scheffer, Marten, Stephen R. Carpenter, Timothy M. Lenton, Jordi Bascompte, William Brock, Vasilis Dakos, Johan Van De Koppel, Ingrid A. Van De Leemput, Simon A. Levin, Egbert H. Van Nes, Mercedes Pascual, and John Vandermeer. 2012. Anticipating Critical Transitions. Science 338 (6105): 344-348.

Schelling, Thomas C. 1960. Strategy of Conflict. Harvard University Press.

Schelling, Thomas C. 1966. Arms and Influence. New Haven: Yale University Press.

Schwartz, Norton A., and Jonathan W. Greenert. 2012. Air-Sea Battle: Promoting Stability in an Era of Uncertainty. The American Interest (20 February).

Shultz, George P., Sidney D. Drell, and James E. Goodby. 2011. Deterrence: Its Past and Future. Stanford, CA: Hoover Institution Press.

Slantchev, Branislav. 2011. Military Threats: The Costs of Coercion and the Price of Peace. New York, NY: Cambridge University Press.

Snook, Scott. 2000. Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq. Princeton: Princeton University Press.

Snyder, Glenn H. 1965. The Balance of Power and the Balance of Terror. In The Balance of Power, ed. Paul Seabury. San Francisco: Chandler.

Snyder, Glenn. 1961. Deterrence and Defense: Toward a Theory of National Security. Westport, CT: Greenwood Press.

Stokes, Mark A. 2012. The Second Artillery Force and the Future of Long-Range Precision Strike. In Ashley J. Tellis, and Travis Tanner (Eds.), Strategic Asia 2012-13: China’s Military Challenge. Seattle, WA: National Bureau of Asian Research.

Stone, John. 2012. Conventional Deterrence and the Challenge of Credibility. Contemporary Security Policy 33(1): 108-123.

Trachtenberg, Marc. 1991. History and Strategy. Princeton, NJ: Princeton University Press.

Van Evera, Stephen W. 1999. Causes of War: Power and the Roots of Conflict. Cornell University Press.

Van Tol, Jan, Mark Gunzinger, Andrew Krepinevich, and Jim Thomas. 2010. Airsea Battle: A Point-Of-Departure Operational Concept. Washington DC: Center for Strategic and Budgetary Assessments.

Wagner, R. Harrison. 2007. War and the State: The Theory of International Politics. Ann Arbor, MI: University of Michigan Press.

Waltz, Kenneth N. 1979. Theory of International Politics. Boston, MA: McGraw-Hill.

Weick, Karl E. 1987. Organizational Culture as a Source of High Reliability. California Management Review 29(2): 112-27.

Weick, Karl E., and Karlene H. Roberts. 1993. Collective Mind in Organizations: Heedful Interrelating on Flight Decks. Administrative Science Quarterly 38(3): 357-81.

Wohlstetter, Albert. 1958. The Delicate Balance of Terror. RAND Occasional Paper (P-1472).